[0001]
[Field of the Invention]The radio communications system with which wireless LAN was used for this invention, the radio terminal which constitutes this radio communications system, A base transceiver station, and registration and the authentication method of this radio communications system are started, and it is especially related with the registration and authentication technology between radio terminals, and the base transceiver station and radio terminal in wireless LAN systems, such as IEEE802.11.
[0002]
[Description of the Prior Art]The network of office environment is advancing considering connection between PCs (Personal Computer) as a center with development of LAN (Local Area Network) art in recent years. Apart from such spread of cable LAN, wireless LAN-ization replaced on radio is also following a part of cable LAN. For example, it is a case where connect a base transceiver station to cable LAN, and two or more portable PCs are connected to this base station on radio. If the file of desktop PC by which Ethernet (registered trademark) connection is made is edited into cable LAN using this portable PC, radio access will be performed to cable LAN. If the portions of a base station and portable PC are started, the portion will form wireless LAN. As an advantage of such wireless LAN, since an electric wave, infrared rays, etc. are used as a transmission line, a point with easy point which does not need wiring construction, network new construction, and layout change is mentioned.
[0003]Introduction of such wireless LAN has required the spur by standardization of IEEE802.11. In IEEE802.11, the wireless LAN specification of a 2.4GHz bandwidth will be completed in 1997, and the wireless LAN specification of a 5GHz bandwidth is completed in 1999, respectively. The access speed of the wireless LAN specification of a 2.4GHz bandwidth has a thing of 1 - 2Mbps, and a thing of 11Mbps, and the specification exceeding 20Mbps is examining it further now. Recently, the product based on this 2.4GHz bandwidth specification comes to be put on the market from each company, and the base station and the radio PC card have been going into the spread price range. On the other hand, in the wireless LAN specification of a 5GHz bandwidth, the access speed of 20 - 30Mbps is realizable. Since the more nearly high-speed access speed which is an almost intact frequency band of only being used for the weather radar now can expect a 5GHz bandwidth easily unlike a 2.4GHz bandwidth, it is expected that it is next-generation wireless LAN specification.
[0004]It comes here, and Bluetooth involves in a cell phone market, and household electrical products industry and PC industry, and is going to be carried in all apparatus. Although this Bluetooth is also a wireless system of a 2.4GHz bandwidth, global spread is suddenly expected from low cost called one about 5-dol tip and having obtained approval from about 2000 companies of a broad type of industry.
[0005]From the above situations, it is thought that spread follows a wireless LAN system not only to office environment but to an ordinary home. Therefore, the near wireless LAN system of plurality in the future adjoins, or it is expected that the environment where it lives together to the same space is built widely.
[0006]By the way, the authenticating processing between radio terminals and between a base transceiver station and a radio terminal is prescribed by IEEE802.11 (Chapter 8 of IEEE802.11 specifications). The method in which two entities (radio terminals, or a base transceiver station and a radio terminal) which are the targets of authenticating processing

attest and carry out secrecy communication using the same secret key (common key) is described by this regulation (however, this authenticating processing is treated as an option). The algorithm called WEP (Wired Equivalent Privacy) is used for this authenticating processing. distribution of a secret key is beforehand performed by a secure method -- only -- it is indicated. Since a secret key corresponds to each of two entities, if it sees from a certain radio terminal, it is necessary to have a secret key for every radio terminals of other in a system, and the secret key of the square order of the number of radio terminals is needed by the whole system.

[0007]Here, it describes briefly [the encryption and decryption by a WEP algorithm]. And the attestation using this WEP algorithm is also described. Drawing 31 is an explanatory view of encryption processing of the WEP algorithm of IEEE802.11. In drawing 31, the processing as which the data transmitted is enciphered is shown and the data transmitted is especially called plaintext PT here.

[0008]First, in the transmitting side, CRC is generated from this PT. That is, ICV is generated. On the other hand, the key sequence KS is generated through a WEP random number generator from the secret key Sk and the initial vector IV. After doubling the connection result {PT, ICV} and length of PT and ICV, exclusive mathematics developed in Japan of this KS is carried out. The result of this exclusive mathematics developed in Japan is cryptogram ET. And the WEP frame shown in drawing 32 consists of doubling a control code with this ET and IV. Secrecy communication by a WEP algorithm is performed by this WEP frame.

[0009]The contents of the decoding processing of the WEP algorithm of IEEE802.11 are shown in drawing 33. The processing which decrypts the received encryption data is shown by drawing 33.In drawing 33, if a receiver receives the WEP frame, IV will be taken out from the WEP frame, it will input into a WEP random number generator with the secret key Sk, and the key sequence KS will be generated. As for this key sequence KS, if IV is not altered, the same thing as KS of drawing 31 should be generated. If exclusive mathematics developed in Japan of this KS is carried out to cryptogram ET in a frame, the plaintexts PT and ICV will be decoded. CRC check of this PT is carried out, and the rightness of PT is checked by comparing ICV' which is that result with decoded ICV. If ICV' and ICV are equal, it will mean succeeding in reception of PT.

[0010]The sequence chart of the authenticating processing by the WEP algorithm of IEEE802.11 is shown in drawing 34. Drawing 34 shows the example which carries out radio between the radio terminals (terminal) in the wireless zone of a base transceiver station (base station) and this base station. In drawing 34, the secret key Sk of each other which is a common key is beforehand exchanged between the base station and the terminal (Step S1001). And a terminal sends the frame of an authentication demand to a base station by radio first (Step S1002). Demanding attestation by a common key system is written down in this authentication demand frame. The secret key Sk is ending with distribution in a base station and the both sides of a terminal at the above-mentioned step S1001.

[0011]Next, if a base station is in the status of authentication demand acceptance, it will create examination sentence CT through a WEP random number generator from the initial vector IV which made it generate in this secret key Sk and inside (Step S1003). Usually, the length of this CT is 128 bytes. A base station carries out radio of the created CT to a terminal (Step S1004).

[0012]A terminal treats as a plaintext CT received from the base station, and enciphers it with the secret key Sk by the method shown in above-mentioned drawing 31 (Step (Sk (CT)) S1005). And a terminal carries out radio of the cryptogram containing this Sk (CT) to a base station (Step S1006).
[0013]Finally the cryptogram sent from the terminal is verified in a base station (Step S1007), and if right, the completion frame of attestation of success status will be sent towards a terminal. On the other hand, if not right, the frame of failure status is sent (Step S1008). This verification is performed by investigating whether Sk (Sk (CT)) (=CT') which is the result of decoding Sk (CT) by the method shown by above-mentioned drawing 33, and CT which the base station created first are the same.
[0014]
[Problem(s) to be Solved by the Invention]As mentioned above, the case where two or more wireless LAN systems adjoin, or it lives together to the same space in a general home with the spread of wireless LAN systems may happen. Here, the case where the domestic radio communications system is installed in two adjoining houses in collective housing illustrated to drawing 1, A houses, and each of B houses is considered.
[0015]In the example of drawing 1, the base transceiver station A is installed in A house, and the base transceiver station B is installed in B house, respectively. However, the cover area of the base stations A and B has a possibility of enough that each base station A and B was installed and of overflowing the houses A and B. For example, if it sees from the base station A of A house, not only the terminals 1 and 3 belonging to A house but the outdoor terminal 2 and the terminal 4 of B house have existed in the cover area of the base station A. However, since the outdoor terminal 2 and the terminal 4 of B house are not terminals belonging to A house, even if the base station A has registration and an authentication demand from the terminals 2 and 4, they do not need to give attestation to the terminals 2 and 4. That is, the terminals which the base station A should attest are only the terminals 1 and 3 which are terminals of A house. Therefore, it is made for the base station A to want to manage registration and attestation of a terminal so that attestation may not be given other than the terminal 1 of A house, and 3. The same thing can be said also in the base station B of B house.
[0016]Even if it is between different manufacturing makers, the interconnectivity of apparatus is required of domestic apparatus. What is necessary is just to perform distribution of a secret key at Step S1001 of drawing 34 at wireless LAN like IEEE802.11 by which proprietary specification is permitted. For example, what is necessary is just to make a secret key to a base station or a terminal beforehand. However, in a domestic radio communications system, the mechanism in which a secret key is exchangeable between the devices of a different maker is needed separately by the secure one and easy method by radio.
[0017]this invention is accomplished in view of this situation, and comes out. The purpose is a radio communications system of **, and is providing the radio communications system which can be performed certainly and easily for the registration and attestation between radio terminals, and a base transceiver station and a radio terminal.

[0018]
[Means for Solving the Problem]It will be as follows if an outline of a typical thing is

explained among inventions indicated here. Namely, in registration and an authentication method for said base transceiver station of said radio terminal in a radio communications system which changes from this base transceiver station and a radio terminal which performs radio to a base transceiver station and this base transceiver station by ending with registration / attestation, (a) stage; (b) which changes the mode of said base transceiver station from the normal mode to register mode because a user operates said base transceiver station -- because said user operates said radio terminal. Change the mode of said radio terminal from the normal mode to register mode, and. If the stage;(c) aforementioned base transceiver station which transmits application-for-registration information containing a cipher system of a public key peculiar to said radio terminal and this public key and an identification number of said radio terminal from said radio terminal to said base transceiver station receives said application-for-registration information, Said base transceiver station enciphers using said terminal public key and a terminal cipher system, and registration-confirmed information which shows a registration permission of said radio terminal is transmitted to said radio terminal, When said radio terminal is able to decode registration-confirmed information by which the stage; (d) aforementioned encryption which changes the mode of said base transceiver station from register mode to authentication mode was carried out using a terminal secret key corresponding to said terminal public key, A stage which changes the mode of said radio terminal from register mode to authentication mode; After the mode of the (e) aforementioned radio terminal shifts to authentication mode, A common key with said base transceiver station peculiar to said base transceiver station, Said base transceiver station enciphers authentication notification information containing a cipher system of this common key, and an identification number of said base transceiver station using said terminal public key and a terminal cipher system. When said radio terminal is able to decode authentication notification information by which the stage; (f) aforementioned encryption which transmits to said radio terminal was carried out using said terminal secret key, Said radio terminal enciphers using said base station common key and a base station cipher system, and attestation received information which shows receipt of said authentication notification information is transmitted to said base transceiver station, When said base transceiver station is able to decode attestation received information by which the stage; (g) aforementioned encryption which changes the mode of said radio terminal from authentication mode to the normal mode was carried out using said base station common key, They are registration and an authentication method including a stage which changes the mode of said base transceiver station from authentication mode to the normal mode.

[0019]In registration and an authentication method concerning this invention, when performing registration and attestation of a radio terminal to a base transceiver station installed, for example in a home, the user of a radio terminal has to do the direct control of the base transceiver station. For this reason, registration and attestation of a radio terminal of a user of the exterior for which operation of a base transceiver station is not easy can be prevented. Thereby, processing of registration and attestation secure one despite radio and easy is realizable.

[0020]

[Embodiment of the Invention]Hereafter, an embodiment of the invention is described in detail, referring to drawings. The main objects of this invention are domestic radio

communications systems. In this system, in a management top, a base transceiver station performs registration and attestation of a radio terminal, and the usual data communications are directly performed between terminals. It is a premise that a terminal has a cipher system by a public-key crypto system, and its secret key and public key. As a public-key crypto system, RSA encryption technology and a elliptic curve cryptosystem method are held, for example. It is a premise that a base station has a cipher system by a common key encryption system and its common key. As a common key encryption system, a DES method, an AES method, etc. are held, for example.

[0021]In this invention, first, it registers with the public-key crypto system of a terminal, next attests with the common key encryption system of a base station. Therefore, the terminals which the same wireless communication system as the usual data was used for this invention, and the base station registered and attested the terminal, and received attestation as a result can carry out secrecy communication in a system with the common key system of a manages base station. By this invention, the external terminal which has not received attestation can prevent spoofing as monitoring the communication in a system, and a terminal in a system. This invention can also be used as a prior distribution method of the secret key for data communications which is the requisite in the WEP algorithm of IEEE802.11.In this case, a WEP algorithm will perform terminal attestation as IEEE802.11 after use of this invention method.

[0022]A base station only takes the responsibility on management of a domestic radio communications system, and is the same as other terminals in the other function at all. Conversely, if it says, when registration and the authentication function of a terminal will be called a base station function, a terminal with this base station function is able to become a base station, and this view passes also to IEEE1394. For this reason, for example, as shown in drawing 1, "a terminal (terminal 5)" and the base station B can also be treated for the base station A as "a terminal (terminal 6)."

[0023]Hereafter, the radio communications system concerning an embodiment of the invention is explained using six examples. The 1st thru/or the 6th example show the case where the terminal 1 is registered and attested to the base station A of drawing 1, respectively. The feature of this invention is at the point of advancing registration and attestation of the terminal, a user checking each state operating both a terminal and a base station. For this reason, registration and attestation of a terminal are realizable secure one despite radio, and easily. That is, the user needs to follow correctly sequences, such as an order of pushing a button, by requiring operation of a terminal or a base station of a user. It is difficult to carry out manual operation of the base station A in a house from the exterior. For this reason, the terminal 2 and the terminal 4 of drawing 1 are fundamentally unable to register with the base station A for example. Even if it should interrupt and should do registration and attestation of the terminals 2 and 4 of these exteriors at the time of registration and attestation of the terminal 1 of A house, or the terminal 3, the user of A house can detect such operation easily by the status display of the base station A, the terminal 1, or the terminal 3.

[0024]The 1st example of the radio communications system concerning an embodiment of the invention is described using the (1st example) next drawing 2, and drawing 3. Drawing 2 is registration / attestation sequence chart of the radio communications system concerning this 1st example. Here, the registration and the authentication sequence (registration and authentication sequence 1) between the base station A of drawing 1

(terminal 5) and the terminal 1 are shown. This registration and authentication sequence 1 are roughly divided, and is divided into a registration stage and an attestation stage. In drawing 2, the time t shall pass from a top to the bottom. Also in the sequence of other below-mentioned examples, these are the same. Drawing 3 focuses on the information exchanged between the base station A and the terminal 1, and explains registration and the authentication sequence 1 of drawing 2. The round enclosure number shown in drawing 3 shows the order of advance of registration and the authentication sequence 1. In this registration and authentication sequence 1, radio of application-for-registration information and the attestation received information is carried out from the terminal 1 to the base station A. Radio of registration-confirmed information and the authentication notification information is carried out from the base station A to the terminal 1. Hereafter, with reference to drawing 2, this registration and authentication sequence 1 are explained.
[0025]The base station A has ** normal mode, ** register mode, and ** authentication mode. The terminal 1 also has the normal mode, i.e., the unregistered normal mode and the registered normal mode, ** register mode, and ** authentication mode of **2 kind. Of course, the number of the normal modes may be one like the base station A. When the number of the normal modes is two, registration of the terminal 1 is limited only at once and the registration of it to one set only of a base station is attained as a result. On the other hand, when the number of the normal modes is one, it can register with two or more base stations. It is because registration of the terminal 1 is not limited at once. In drawing 2, the next notation is used about the LED display of the base station A and the terminal 1. "R" is a red light and expresses register mode. "G" is green lighting and expresses the registered normal mode. "<R>" is red blink and expresses authentication mode. "<G>" is green blink and expresses the unregistered normal mode. Otherwise, the example of a LED display can consider a variation. For example, authentication mode is yellow lighting etc. The base station A of drawing 2 and the right triangle display of the terminal 1 express button grabbing by a user.
[0026](a) A user changes the mode of the base station A from the normal mode to register mode by operation of the registering button of the base station A first (the time a, Step S101). The timer 1 starts at this time.
[0027](b) Next, a user pushes the registering button of the terminal 1 (the time b, Step S102). According to the operation, the terminal 1 carries out wireless transmission of the application-for-registration information to the base station A (Step S103). When the registering button of the terminal 1 is pushed, the timer 3 starts. The mode of the terminal 1 also changes from the normal mode to register mode after transmission of this application-for-registration information. It means that both the base station A and the terminal 1 had shifted to register mode at this time.
[0028]As shown in drawing 4, the MAC Address of the terminal 1, the public key of the terminal 1 and a public-key crypto system, and its information peculiar to end of the other end 1, including apparatus classification, a serial number, a manufacturing-company name, a user name, etc., are included in the application-for-registration information which the terminal 1 transmits. As a MAC Address, the EUI 64 address or EUI 48 address of IEEE can be considered. It is because the terminal 1 can be specified as a meaning according to these addresses. An EUI 64 address is divided into 24 bits of the first half, and 40 bits of the second half, a first half is CompanyID assigned by IEEE and the company to which this CompanyID was assigned can use the latter half freely. For

example, an address called AC-DE-64-00-00-00-00-80 (hexa display) is shown. In IEEE1394, EUI64 is used as an address peculiar to a node (terminal). An EUI 48 address is used by the Ethernet address etc., and if it removes the point that the latter half is 24 bits, it is almost the same as EUI64. With an EUI 64 address, if the first two octets of the latter half are set as FF-FE (hexa display), it can be used as EUI48 address format.
[0029]The terminal 1 holds beforehand the public key and the public-key crypto system. These are written in ROM etc. which were carried in terminal 1 self at the time of product shipment, for example, or are written in ROM of the radio interface card of the terminal 1.
[0030]As an example of terminal 1 characteristic data, information, including the classification and the serial number of apparatus, a manufacturing-company name, a user's name, etc., can be considered. These information may be coded and managed. For example, apparatus classification is expressed by 4 bits, 0000 decides on wireless TV, 0001 decide on digital VCR, and 0010 should just decide on the notebook PC etc. In 00000, Toshiba and 00001 should just also assign the manufacturing-company name beforehand with Sony etc.
[0031](c) The base station A returns registration-confirmed information to the terminal 1, when the application-for-registration information from the terminal 1 is received (the time c, Step S104). This registration-confirmed information reports that the terminal 1 was able to be registered by the base station A side to the terminal 1 side. At this time, the mode of the base station A changes from register mode to authentication mode. The timer 2 is also started. Registration-confirmed information is enciphered by the public key of the terminal 1 received from the terminal 1 using application-for-registration information. By this encryption, only the terminal 1 which required the application for registration can read the contents of registration-confirmed information. As shown in drawing 5, the MAC Address of the flag which shows that registration is O.K., and the terminal 1 which is the objects of the registration O.K., terminal inherent information, etc. are included in this registration-confirmed information. Such terminal MAC Addresses, terminal inherent information, etc. are acquired from the application-for-registration information on above-mentioned drawing 4.
[0032](d) By acceptance of the registration-confirmed information from the base station A, the mode of the terminal 1 changes from register mode to authentication mode (time d). The timer 4 starts at this time.
[0033](e) The base station A transmits authentication notification information to the terminal 1 after the time progress beforehand defined from the shift point in time (time c) to authentication mode (the time e, Step S105). The relation of this time e and time d is considered so that an authentication notification can be received, when the terminal 1 is certainly in authentication mode. As shown in drawing 6, an authentication notification, the MAC Address of the base station A, the common key of the base station A and a common key encryption system, and the characteristic data of the base station A are included in authentication notification information. And it is enciphered like registration-confirmed information using the public key and public-key crypto system of the terminal 1. Since only the terminal 1 has a public key and a pair of secret key, the other terminal cannot check the authentication notification information on the terminal 1.
[0034](f) The terminal's 1 acceptance of authentication notification information will reply attestation received information to the base station A (the time f, Step S106). At this time,

the mode of the terminal 1 changes from authentication mode to the normal mode (green lighted indication). The terminal 1 which was the unregistered normal mode (green blink) serves as the registered normal mode (green lighting) at the beginning [of registration and authenticating processing]. On the other hand, the base station A which was the normal mode (green lighted indication) returns at the beginning. Attestation received information includes that the terminal 1 received the authentication notification (attestation O.K.) with the terminal address and base station MAC Address of the terminal 1, as shown in drawing 7. It is enciphered with the common key and common key encryption system of the base station A, and these are transmitted to the base station A.

[0035](g) The base station A returns from authentication mode to the normal mode, when the attestation received information from the terminal 1 is able to be decoded correctly (time g). When the terminal 1 and the base station A are the normal mode at the time g at this time, this terminal 1 is registered and attested by the base station A, and processing completes it.

[0036]Thus, the terminal 1 registered and attested becomes possible [using the common key encryption system of the base station A], and comes to be able to carry out secrecy communication with other attested terminals in the domestic radio communications system which the base station A manages. For example, as shown in drawing 8, the commo data between terminals is kept secret. That is, the base station A is the example which is carrying out domestic radio communications system management, and the base station A has enciphered drawing 8 using the common key SKsa held beforehand and its cipher system SAsa. In this case, unless registration and attestation are received from the base station A, each terminal cannot read this secrecy commo data.

[0037]Drawing 9 is a figure showing the contents of the registration authentication table managed by the base station A. A MAC Address, a public key, a cipher system, terminal inherent information, etc. are recorded on this registration authentication table for every terminal. The data for every terminals of these is obtained from the application-for-registration information on each terminal illustrated to above-mentioned drawing 4. Of course, in this table, the information on base station A itself is also included. As information on base station A itself, the common key which the base station A holds beforehand, and its common key encryption system are held. When the base station A functions as a terminal, the public key by the MAC Address and public-key crypto system which are required information, a secret key and its cipher system, and other terminal inherent information are included.

[0038]It is possible to handle failure in registration and attestation and to return the base station A and the terminal 1 to the normal mode in the 1st above-mentioned example, using the timer (the timer 1 - the timer 4) of drawing 2. Hereafter, operation of the timer in this case is explained using drawing 10 thru/or drawing 14.

[0039](1) Drawing 10 is a sequence chart at the time of the ability for the base station A not to receive this information well, and not reply registration-confirmed information as a result, although the terminal 1 transmitted application-for-registration information to the base station A. In this case, in the base station A, although the timer 1 started at the time a, the deadline is passed at the time c and it returns to the original normal mode. With the reply of application-for-registration information not got, i.e., registration-confirmed information, although the timer 3 also started one terminal 1 at the time b, it passes the

deadline at the time d and returns to the original normal mode. Since the base station A and the terminal 1 also return to the normal mode, without going into authentication mode, having failed can judge them visually. If the time limit of the timer 1 and the timer 3 is set up for a long time than the time which registration and attestation take, the length of the time can also be made into a visual judgment source.

[0040](2) Drawing 11 is a sequence chart when the terminal 1 is not able to decode correctly the registration-confirmed information from the base station A. In this case, since the terminal 1 cannot receive registration-confirmed information correctly, the timer 3 will pass the deadline and the mode of the terminal 1 will return to the original normal mode. As a result, since the base station A cannot receive attestation received information from the terminal 1, the timer 2 passes the deadline similarly and the mode of the base station A will also return to the original normal mode.

[0041]The timer 1 of the base station A is normally canceled at the time c which sent out registration-confirmed information to the terminal.

[0042](3) Drawing 12 is a sequence chart when the terminal 1 is not able to receive correctly the authentication notification information from the base station A. That is, the base station A is to usually transmit authentication notification information to the terminal 1 after certain time progress from start time [of the timer 2] c, as shown in above-mentioned drawing 2. However, the case where transmission to the terminal 1 of this authentication notification information fails in a certain reason is assumed. In this case, the base station A cannot receive attestation received information from the terminal 1 as a result of the receiving failures of authentication notification information. For this reason, the timer 2 passes the deadline and the mode of the base station A will return to the original normal mode. On the other hand, authentication notification information cannot be received from the base station A, but the timer 4 passes the deadline, and the terminal 1 returns to the original normal mode.

[0043]The timer 1 of the base station A is the time c which sent out registration-confirmed information to the terminal 1, and is canceled normally. The timer 3 of the terminal 1 is also normally canceled at the time d which has decoded registration-confirmed information correctly.

[0044](4) Drawing 13 is a sequence chart when the terminal 1 is not able to decode correctly the authentication notification information from the base station A. In this case, the terminal 1 cannot receive authentication notification information from the base station A correctly like the case of above (3). For this reason, the timer 4 passes the deadline and the terminal 1 returns to the original normal mode. On the other hand, like above (3), attestation received information cannot be received from the terminal 1, but the timer 2 passes the deadline, and the base station A returns to the original normal mode.

[0045]The timer 1 of the base station A is the time c which sent out registration-confirmed information to the terminal 1, and is canceled normally. The timer 3 of the terminal 1 is also normally canceled at the time d which has decoded registration-confirmed information correctly.

[0046](5) Drawing 14 is a sequence chart when the base station A is not able to decode attestation received information from the terminal 1 correctly. In this case, since the base station A cannot decode attestation received information from the terminal 1, the timer 2 passes the deadline and returns to the original normal mode. On the other hand, since the terminal 1 received correctly the authentication notification information from the base

station A, it returns to the original normal mode as normal operation. Decoding failure of the attestation received information of the base station A will be detected by the deadline of the timer 2. When the time limit of this timer 2 is set up for a long time than the time of normal termination, decoding or failure of attestation received information can be judged according to increase of time to stay at the authentication mode of the base station A.

[0047]The timer 1 of the base station A is the time c which sent out registration-confirmed information to the terminal 1, and is canceled normally. The timer 3 of the terminal 1 is also normally canceled at the time d which has decoded registration-confirmed information correctly. The timer 4 of the terminal 1 is also normally canceled at the time f which sent out attestation received information to the base station A.

[0048]In above (1) thru/or (4), when the normal mode of the terminal 1 is divided into the unregistered normal mode and the registered normal mode and registration and attestation go wrong, the terminal 1 will return to the unregistered normal mode. In this case, compared with the case where the number of the normal modes is one, it enables a user to judge more visually.

[0049]In the 1st above-mentioned example, only one terminal can receive registration and attestation depending on one registration and an authentication sequence. Hereafter, this point is explained using drawing 15. In the example of drawing 15, since the direction of the terminal 2 pushed the registering button earlier than the terminal 1 (Step S102, step S102'), the application-for-registration information on the terminal 2 was received (Step S103, step S103'), and registration and attestation were able to be received as the result. The time of pushing a registering button, although one terminal 1 was register mode, the timer 1 passed the deadline at the time te, and it has returned from ts to the normal mode. Since it did not go into authentication mode, registration and the authentication failure of the terminal 1 can be judged to be the deadlines of this timer 1. Thus, when a base station makes application-for-registration information to receive during a register mode period and receive only the registration and the authentication demand from one terminal, it will be guaranteed that registration and attestation of a terminal are only one terminal simultaneously. Since registration and having attested can also presume the terminal of other houses or the exterior accidentally according to this, registration and attestation of a terminal can be redone. For example, suppose that the terminal 1 of drawing 15 is an internal terminal, and the terminal 2 is an external terminal. In this case, although the internal terminal 1 went wrong, since it is quite obvious that the base station is following the right sequence, it can be judged that registration and attestation of a certain terminal (here external terminal 2) may have been done accidentally. Thus, by the ability to judge, it is possible to redo registration and attestation of the internal terminal 1, or to correct the registration authentication table (refer to drawing 9) of a base station. The correction of the registration authentication table of a base station can perform deletion of only the latest information, deletion of all the information, etc.

[0050]In the 1st above-mentioned example, the sequence which serves as transmission (Step S104) of the registration-confirmed information on drawing 2 and transmission (Step S105) of authentication notification information is also considered. In this case, the base station A will be replied, after combining the registration-confirmed information on drawing 5, and the authentication notification information on drawing 6 and enciphering

by the public key and encryption algorithm of a public-key crypto system of the terminal 1, when the application-for-registration information from the terminal 1 is received. When this registration confirmed and authentication notification are received, the mode of the terminal 1 shifts to authentication mode. Attestation received information is created in the midst of this authentication mode. And when attestation received information is transmitted to the base station A, the terminal 1 changes to the normal mode.

[0051]After operating the registering button of the base station A, according to the 1st above-mentioned example, before the timer 1 of the base station A times out, it is necessary to operate the registering button of the terminal 1, as explained above. For this reason, operating the base station A in a house from the outside can process registration and attestation secure one despite radio, and easy together with a difficult thing.

[0052]The 2nd example of the radio communications system concerning an embodiment of the invention is described using the (2nd example) next drawing 16, and drawing 17. Drawing 16 is registration / attestation sequence chart of the radio communications system concerning this 2nd example. The point that registration and the authentication sequence of drawing 16 (registration and authentication sequence 2) differ from registration and the authentication sequence 1 of the 1st above-mentioned example is a point of pushing an authentication button clearly, when the base station A sends authentication notification information at the time e (Step S206) (Step S205). This authentication button may be independently arranged with a registering button, and may be the same button. When it constitutes from same button, and pushes short (for example, less than 1 second) and pushes for a long time (for example, several seconds) with a registering button, it is good also as an authentication button. In addition, various variations can be considered. Anyway, if an authentication button is used in this way, after a user will check that the terminal has changed from the register mode to authentication mode, authentication operation can be clearly started with an authentication button. Therefore, a user can recognize easily the registration stage having been completed and having gone into the attestation stage rather than registration and the authentication sequence 1 of the 1st above-mentioned example.

[0053]The timer (the timer 1, the timer 2, the timer 3, the timer 4) of drawing 16 is the same as that of registration and the authentication sequence 1 of drawing 2 except for the point that the starts of the timer 2 differ. The use of a timer is the same as the sequence 1, and it operates like drawing 10 thru/or drawing 14. The timer 2 of the base station A of drawing 16 is started from the time of a user pushing the authentication button of the base station A. It is canceled when attestation received information is able to be decoded correctly, and it is canceled in the place which exceeded the time limit at the time of the other abnormalities.

[0054]Drawing 17 focuses on the information exchanged between the base station A and the terminal 1, and explains registration and the authentication sequence 2 of drawing 16. The round enclosure number of drawing 17 shows the order of advance of registration and the authentication sequence 2. In this registration and authentication sequence 2, radio of application-for-registration information and the attestation received information is carried out from the terminal 1 to the base station A. On the other hand, radio of registration-confirmed information and the authentication notification information is carried out from the base station A to the terminal 1.

[0055]Since this 2nd example is clear in correlation with an authentication notification and the change rate to the authentication mode of a terminal compared with the 1st above-mentioned example, its point that the registration and attestation which the terminal which is not a request mistook can be prevented is advantageous. In the example of drawing 11 described in the 1st example, drawing 13, and drawing 14, it may be because it was attested [registration and] accidentally [terminal / with an another failure in registration and attestation of the terminal 1]. This is because the terminal 1 cannot grasp reply timing of the authentication notification from the base station A. On the other hand, after checking that the terminal 1 has become authentication mode in this 2nd example, in order that a user may operate the authentication button of the base station A, this reply timing is clear. Therefore, the base station A can prevent registration and the thing to attest accidentally [terminal / another].
[0056]As explained above, according to this 2nd example, before operating the registering button of the base station A and the timer 1 of the base station A times out, after it is necessary to operate the registering button of the terminal 1 and and the terminal 1 changes to authentication mode, it is necessary to operate the authentication button of the base station A. For this reason, operating the base station A in a house from the outside can process registration and attestation secure one despite radio, and easy together with a difficult thing.
[0057]The 3rd example of the radio communications system concerning an embodiment of the invention is described using the (3rd example) next drawing 18, and drawing 19. Drawing 18 is registration / attestation sequence chart of the radio communications system concerning this 3rd example. The point that registration and the authentication sequence of drawing 18 (registration and authentication sequence 3) differ from registration and the authentication sequence 2 of the 2nd above-mentioned example is a point that a user pushes clearly not the authentication button of the base station A but the authentication button of the terminal 1 (Step S305). If it does in this way, after a user will check that the terminal 1 has changed from the register mode to authentication mode, an attestation application is made with an authentication button (Step S306), and it becomes operation called attestation receipt through an authentication notification (Step S307) as the result in the direction of the terminal 1 (Step S308). It differs in above-mentioned registration and authentication sequences 1 and 2, and operation of the authentication button of the terminal 1 by a user is performed in this registration and authentication sequence 3 (Step S305). The attestation application information of Step S306 includes an attestation application demand, the MAC Address of the terminal 1, and terminal inherent information, as shown in drawing 20. It is enciphered using the secret key of the public key system of the terminal 1, and these data is transmitted to the base station A from the terminal 1. here -- it should observe -- it is that the secret key of the terminal 1 is used. Therefore, unless it uses this key and the public key which has accomplished the pair, it cannot decode. This is a digital signature by the terminal 1. It can be judged whether it is the attestation application information which the terminal [finishing / registration completion / by the time d] 1 sent out by this digital signature.
[0058]Drawing 19 focuses on the information exchanged between the base station A and the terminal 1, and explains registration and the authentication sequence 3 of drawing 18. The round enclosure number of drawing 19 shows the order of advance of registration and a sequence. In this registration and authentication sequence 3, radio of application-

for-registration information, attestation application information, and the attestation received information is carried out from the terminal 1 to the base station A. Radio of registration-confirmed information and the authentication notification information is carried out from the base station A to the terminal 1.
[0059]Like the 2nd above-mentioned example, since correlation with an authentication notification and the change rate to the authentication mode of a terminal is clear, this 3rd example can prevent the registration and attestation which the terminal which is not a request mistook.
[0060]As explained above, after operating the registering button of the base station A according to this 3rd example, Before the timer 1 of the base station A times out, after it is necessary to operate the registering button of the terminal 1 and and the terminal 1 changes to authentication mode, before the timer 2 of the base station A times out, it is necessary to operate the authentication button of the terminal 1. For this reason, operating the base station A in a house from the outside can process registration and attestation secure one despite radio, and easy together with a difficult thing.
[0061]The 4th example of the radio communications system concerning an embodiment of the invention is described using the (4th example) next drawing 21, and drawing 22. Drawing 21 is registration / attestation sequence chart of the radio communications system concerning this 4th example. Drawing 22 focuses on the information exchanged between the base station A and the terminal 1, and explains registration and the authentication sequence of drawing 21 (registration and authentication sequence 4). The round enclosure number shown in drawing 22 shows the order of advance of registration and the authentication sequence 4. In this registration and authentication sequence 4, radio of application-for-registration information, attestation application information, and the attestation received information is carried out from the terminal 1 to the base station A. Radio of registration received information, registration-confirmed information, and the authentication notification information is carried out from the base station A to the terminal 1. Hereafter, with reference to drawing 21, this registration and authentication sequence 4 are explained.
[0062](a) A user pushes the registering button of the terminal 1 first (the time a, Step S401). That is, it shifts to register mode (a LED display is a red light) previously from the direction of the terminal 1. The timer 3 starts at this time.
[0063](b) Next, a user pushes the registering button of the base station A (the time b, Step S402). If a registering button is pushed, the base station A will transmit the registration received information shown in drawing 23 to the terminal 1 (Step S403). At this time, the base station A shifts to register mode, and that LED display serves as a red light. The timer 1 is also started simultaneously. As shown in drawing 23, the flag which shows registration reception ****, and a base station MAC Address are contained in registration received information.
[0064](c) If the terminal 1 receives the registration received information from the base station A, the terminal 1 will transmit shortly the application-for-registration information shown in above-mentioned drawing 4 to the base station A (Step S404).
[0065](d) If the base station A receives the application-for-registration information from the terminal 1, the base station A will transmit the registration-confirmed information shown in above-mentioned drawing 5 to the terminal 1 (Step S405). At this time, the mode of the base station A changes from register mode to authentication mode. The timer

1 carries out normal termination, and the timer 2 starts. Since the registration-confirmed information transmitted from the base station A is enciphered by the public key of the terminal 1 which made the application for registration as the 1st above-mentioned example described, only the terminal 1 can read the contents.
[0066](e) The terminal 1 will transmit the attestation application information shown in above-mentioned drawing 20 to the base station A, if the registration-confirmed information from the base station A can be decoded correctly (Step S406). At this time, the mode of the terminal 1 changes from register mode to authentication mode. The timer 3 carries out normal termination and the timer 4 starts. Since it is enciphered using the secret key of the terminal 1, the attestation application information of drawing 20 cannot be decoded unless it uses this key and the public key which has accomplished the pair. This can be considered to be a digital signature by the terminal 1. It can be judged whether by this signature, the terminal 1 in which attestation application information carried out registration completion by the above-mentioned (a) thru/or (d) sends out.
[0067](f) Since the base station A knows the public key of the terminal 1, it can decode the attestation application information from the terminal 1. And the base station A transmits the authentication notification information shown in above-mentioned drawing 6 to the terminal 1 (Step S407). It is enciphered by the public key of the terminal 1, and this authentication notification information is decoded with that key and the secret key which has accomplished the pair.
[0068](g) By this decoding, if the secret key of the base station A, etc. can be taken out correctly, the attestation received information shown in above-mentioned drawing 7 will be transmitted to the base station A (Step S408). At this time, the terminal 1 becomes the normal mode (registered) and carries out normal termination also of the timer 4.
[0069](h) If the attestation received information from the terminal 1 is received in the base station A, the base station A will return to the normal mode, and normal termination also of the timer 2 will be carried out. Here, registration and attestation of the terminal 1 are completed.
[0070]As explained above, unlike the above-mentioned 1st thru/or the 3rd example, this 4th example has the feature that the whole processing is base station A initiative. According to this 4th example, after operating the registering button of the terminal 1, before the timer 3 of the terminal 1 times out, it is necessary to operate the registering button of the base station A. For this reason, operating the base station A in a house from the outside can process registration and attestation secure one despite radio, and easy together with a difficult thing.
[0071]The 5th example of the radio communications system concerning an embodiment of the invention is described using the (5th example) next drawing 24, and drawing 25. Drawing 24 is registration / attestation sequence chart of the radio communications system concerning this 5th example. A different point from registration and the authentication sequence 4 of the 4th example of the above [registration and the authentication sequence of drawing 24 (registration and authentication sequence 5)] is using an authentication button, when the terminal 1 transmits attestation application information to the base station A at the time f. If it does in this way, after a user will check that the terminal 1 has changed from register mode to authentication mode, an attestation application can be made with the authentication button of the terminal 1. Although time and effort of the part of an authentication button increases compared with

above-mentioned registration and authentication sequence 4, it is effective in making a user more conscious of authentication operation.
[0072]Drawing 25 focuses on the information exchanged between the base station A and the terminal 1, and explains registration and the authentication sequence 5 of drawing 24. The round enclosure number of drawing 25 shows the order of advance of registration and a sequence. In this registration and authentication sequence 5, radio of application-for-registration information, attestation application information, and the attestation received information is carried out from the terminal 1 to the base station A. On the other hand, radio of registration received information, registration-confirmed information, and the authentication notification information is carried out from the base station A to the terminal 1.
[0073]After operating the registering button of the terminal 1 according to this 5th example, before the timer 1 of the terminal 1 times out, After it is necessary to operate the registering button of the base station A and and the terminal 1 changes to authentication mode, before the timer 2 of the base station A times out, it is necessary to operate the authentication button of the terminal 1. For this reason, operating the base station A in a house from the outside can process registration and attestation secure one despite radio, and easy together with a difficult thing.
[0074]The 6th example of the radio communications system concerning an embodiment of the invention is described using the (6th example) next drawing 26, and drawing 27. Drawing 26 is registration / attestation sequence chart of the radio communications system concerning this 6th example. The point that registration and the authentication sequence of drawing 26 (registration and authentication sequence 6) differ from registration and the authentication sequence 5 of the 5th above-mentioned example is a point of using an authentication button at the time f in the direction of the base station A instead of the terminal 1. By this operation, the base station A transmits the authentication notification information shown in above-mentioned drawing 6 to the terminal 1. The terminal 1 does not need to transmit attestation application information like registration and the authentication sequence 5. That is, after checking that the terminal 1 has changed from register mode to authentication mode, pushing the authentication button of the base station A has replaced transmission of attestation application information. In comparison with registration and the authentication sequence 4 of the 4th example, although time and effort of the part of an authentication button increases, it is effective in making a user more conscious of authentication operation.
[0075]Drawing 27 focuses on the information exchanged between the base station A and the terminal 1, and explains registration and the authentication sequence 6 of drawing 26. The round enclosure number of drawing 27 shows the order of advance of registration and a sequence. In this registration and authentication sequence 6, radio of application-for-registration information and the attestation received information is carried out from the terminal 1 to the base station A. Radio of registration received information, registration-confirmed information, and the authentication notification information is carried out from the base station A to the terminal 1.
[0076]After operating the registering button of the terminal 1 according to this 6th example, before the timer 1 of the terminal 1 times out, After it is necessary to operate the registering button of the base station A and and the terminal 1 changes to authentication mode, before the timer 4 of the terminal 1 times out, it is necessary to

operate the authentication button of the base station A. For this reason, operating the base station A in a house from the outside can process registration and attestation secure one despite radio, and easy together with a difficult thing.
[0077](Base transceiver station) Next, the base transceiver station applied to the radio communications system concerning an embodiment of the invention is explained. Drawing 28 is a block diagram showing the system configuration of the base transceiver station concerning an embodiment of the invention. As shown in drawing 28, this base station 10 is provided with the state set part 101, the status display part 102, the system certification information Management Department 103, the terminal certification information Management Department 104, the timer setting part 105, the Radio Communications Department 106, and the controller 107.
[0078]The state set part 101 is a button of register mode or authentication mode. The status display part 102 is the LED display described in the above-mentioned 1st thru/or the 6th example, for example. as except a LED display, it is based on the instruction display to display screens, such as a liquid crystal, directions by the character string printed by the side of LED, directions with a sound, and a melody -- it displays, and network connection was carried out and also an instruction display on a node screen etc. are considered.
[0079]The system certification information Management Department 103 manages the common key encryption system used within the jurisdiction system of this base station 10. The secret key and cryptographic algorithm of the common key encryption system are managed, and it is necessary to prevent from reading easily from the exterior. At the terminal certification information Management Department 104, terminal inherent information, the public key, and the cryptographic algorithm are managed about the terminal has been attested [registration and] in the system which this base station 10 has jurisdiction over by the registration authentication table shown in above-mentioned drawing 9. The terminal inherent information as a terminal of base station 10 the very thing and the information on a public-key crypto system are also managed.
[0080]The timer setting part 105 has managed the timer of the base station 10 in which it appeared in the above-mentioned 1st thru/or the 6th example, and controls the start and end. The Radio Communications Department 106 is a portion which performs exchange of a terminal and information by radio.
[0081](Radio terminal) Next, the radio terminal applied to the radio communications system concerning an embodiment of the invention is explained. Drawing 29 is a block diagram showing the system configuration of the radio terminal concerning an embodiment of the invention. As shown in drawing 29, this terminal 20 is provided with the state set part 201, the status display part 202, the system certification information Management Department 203, the terminal information Management Department 204, the timer setting part 205, the Radio Communications Department 206, and the controller 207.
[0082]The state set part 201 is a button of register mode or authentication mode like the state set part 101 of drawing 28. The status display part 202 is a LED display like the status display part 102 of drawing 28. The system certification information Management Department 203 saves the common key encryption system in the jurisdiction system of a base station which received registration and attestation. The secret key and cryptographic algorithm of the common key encryption system are managed, and it is necessary to

prevent from reading easily from the exterior like the system certification information Management Department 103 of drawing 28. The terminal information Management Department 204 has managed the characteristic data of this terminal 20, and the information on a public-key crypto system. The timer setting part 205 has managed the timer of the terminal 20 which appeared in above-mentioned Examples 1-6, and controls the start and end. The Radio Communications Department 206 is a portion which performs exchange of a base station and information by radio.

[0083]Now, if registration and the authentication sequences 1 thru/or 6 of the above-mentioned 1st thru/or the 6th example are used, it will have explained that it is possible to register and attest a terminal to the system which a base station manages. The status display according to manual operation, such as a button, LED, etc. like this invention, If a public key system and a common key system are combined, the same radio system as the usual data communications can perform registration and attestation, Since it is difficult for a user to be able to judge easily since the status display of whether whether it succeeded went wrong is carried out, and to carry out manual operation of the base station in a house from the exterior, registration and attestation secure one despite radio and easy can be carried out.

[0084]Two or more base stations are prepared, with a domestic wireless system, if an individual, a group, all families, etc. are arbitrary units and can set up flexibly, it will be thought that it is desirable, but it can respond also to this. For example, it is a case like drawing 30. In one house (it is called X house), the base station A only for Mr. [A], and the base station B only for Mr. [B] and the base station X for all families are installed. The base station A registers and attests only Mr. A's terminal 3. On the other hand, registration and attestation of the outdoor passing terminal 2 in base station A area and the terminal 4 for Mr. [B] are refused. Similarly, only Mr. B's terminal 4 is registered and attested by the base station B. The base station X registers and attests all the terminals in X house, and registers and attests the terminal 3 or not only the terminal 4 but the base station A and the base station B as a terminal. In such a case, the number of the normal modes of a terminal is one, and a terminal can be registered and attested to two or more base stations.In such a case, the secret key and cryptographic algorithm of a common key encryption system of two or more sets ground offices come to be managed by each terminal at a system certification information accumulating part. For example, the secret key and cryptographic algorithm of the base station A and the base station X are managed by the terminal 3.

[0085]

[Effect of the Invention]According to this invention, the radio terminal which can perform certain and easy registration and attestation in a domestic radio communications system, a base transceiver station, a domestic radio communications system, and registration and an authentic method are realizable.